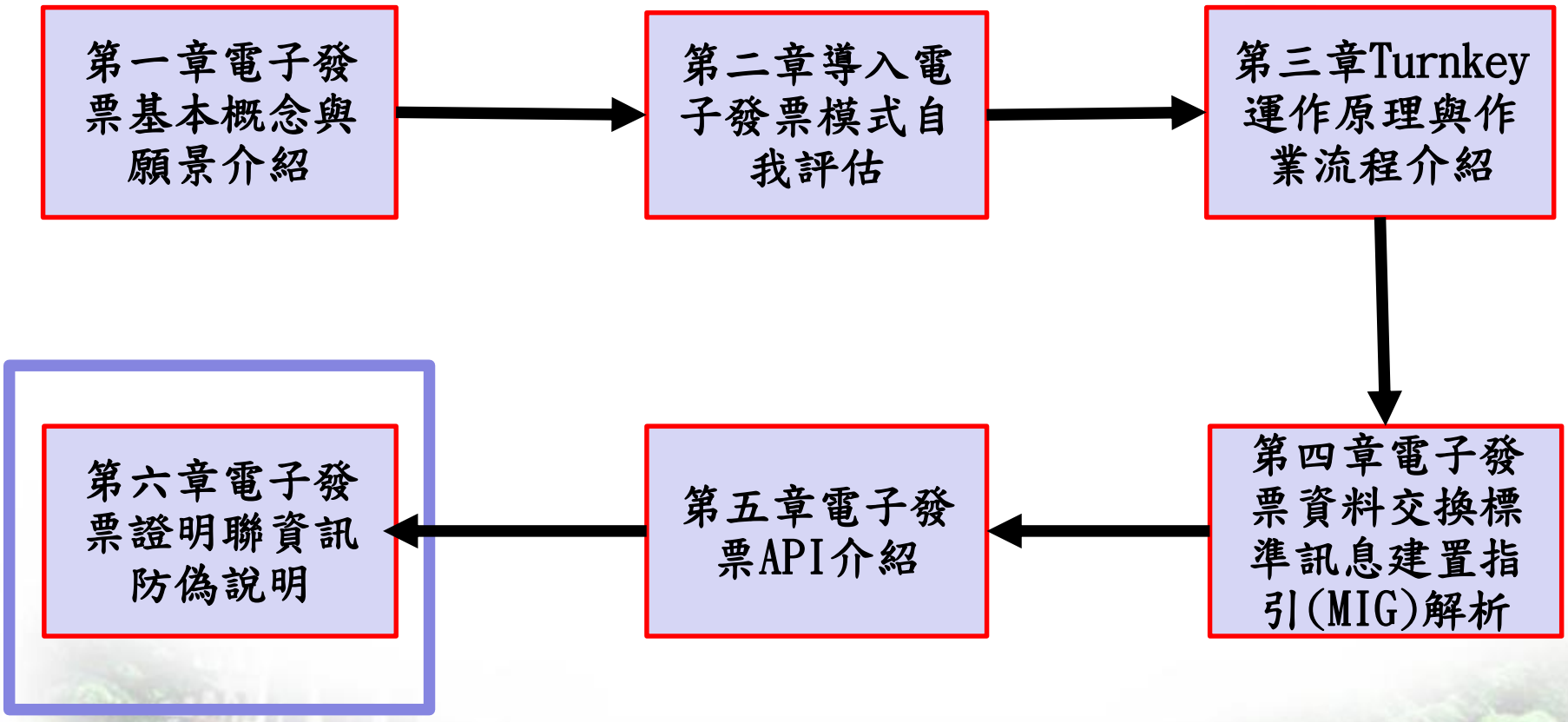
營業人導入電子發票作業指引

第六章電子發票證明聯資訊防偽說明

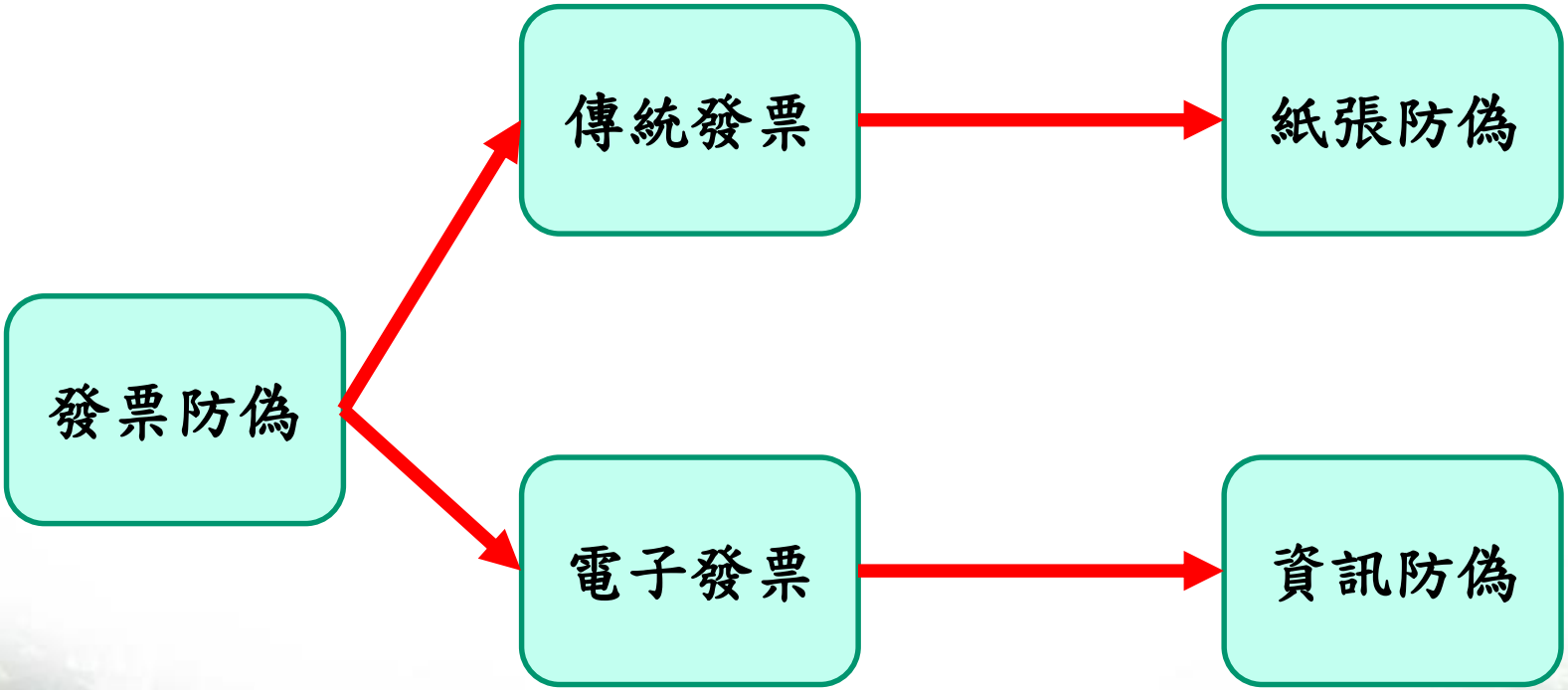

第一章電子發票基本概念與願景介紹
第二章導入電子發票模式自我評估
第三章Turnkey運作原理與作業流程介紹
第四章電子發票資料交換標準訊息建置指引(MIG)解析
第五章電子發票API介紹
第六章電子發票證明聯資訊防偽說明

第六章電子發票證明聯資訊防偽說明

第六章電子發票證明聯資訊防偽說明

本章介紹電子發票證明聯防偽機制，以確保消費者兌領獎權益及推動兌領獎業務。

電子發票證明聯資訊防偽的介紹



電子發票證明聯資訊防偽機制

第一層資訊防偽:隨機碼，為每一張發票的密碼，類似房子大門的鑰匙

第一層資訊防偽:
營業人開立發票隨機給的4位數字

第二層資訊防偽:
加密驗證資訊
第二層資訊防偽:
營業人在平台設定的密碼類似房子內門的鑰匙

第二層資訊防偽要破解之前就需要破解第一層資訊防偽隨機碼
(就像要開啟房子內門除了要有房子內門鑰匙外，就要有房子大門的鑰匙)

發票總項一維條碼

電子發票證明聯資訊防偽的工作為賣方統編當責,發票是賣方統編開立[此張發票顯示為賣方當然是賣方處理資訊防偽]

電子發票證明聯資訊防偽機制

發票總項一維條碼(兌領獎掃描使用)

- 以Code39記載

欄位名稱	長度	說明
發票期別	5	民國年+雙數期別 ex.102年1-2月期發票則填入 10202
發票號碼	10	記載發票號碼，包含字軌2碼+數字8碼
隨機碼	4	四位純數字隨機碼

電子發票證明聯資訊防偽機制

第一層資訊防偽:
營業人開立發票
隨機給的4位數字

第一層資訊防偽:隨機碼，為每一張發票的密碼，類似房子大門的鑰匙

電子發票證明聯資訊防偽機制

第一層資訊防偽:隨機碼之設計建議

- 建議產製規則:每開立一萬張發票不可以重複，開立下一萬張票隨機碼出現的次序不可以重複。
- 例如:開立第1張票之隨機碼為1234 ，開立第10001張之隨機碼不可為1234
- 隨機碼可以說是該發票的密碼，電子發票整合服務平台只要知道發票號碼、發票日期、隨機碼等就可以查詢發票明細

電子發票證明聯資訊防偽機制

第二層資訊防偽:
加密驗證資訊
第二層資訊防偽:
營業人在平台設定
的密碼類似房子
內門的鑰匙

電子發票證明聯資訊防偽機制

第二層資訊防偽:加密驗證資訊

- 第二層資訊防偽:加密驗證資訊可以說是營業人對於所開立發票驗證真偽的設計。
- 通常對於中大獎的獎項會進行第二層資訊防偽驗證。
- 第二層資訊防偽需要先破解第一層隨機碼，與取得營業人在電子發票平台所設定的QRCODE種子密碼。
- 第二層資訊防偽被破解也可以比較該發票之明細，以利區分發票的真偽

電子發票證明聯資訊防偽機制

第二層資訊防偽:
加密驗證資訊
與發票明細

電子發票證明聯資訊防偽機制

欄位名稱	長度	說明
發票號碼	10	記載發票號碼，包含字軌2碼+數字8碼
發票開立日期	7	民國年YYY+MM+DD
隨機碼	4	四位純數字隨機碼
銷售額	8	未稅金額 八碼，將金額轉換以十六進位方式記載。(若營業人銷售系統無法順利將稅項分離計算，則以00000000記載。)
總計額	8	含稅總金額 八碼，將金額轉換以十六進位方式記載。
買方統一編號	8	買受人統一編號 若買受人為一般消費者則以 00000000記載。
賣方統一編號	8	賣方統一編號
加密驗證資訊	24	將發票號碼十碼及隨機碼四碼以字串方式合併後使用 AES加密並採用Base64 編碼轉換(AES所採用之金鑰產生方式另參文件)
總計	77	
以下以冒號「:」間隔，填入發票明細資訊		

電子發票證明聯資訊防偽機制

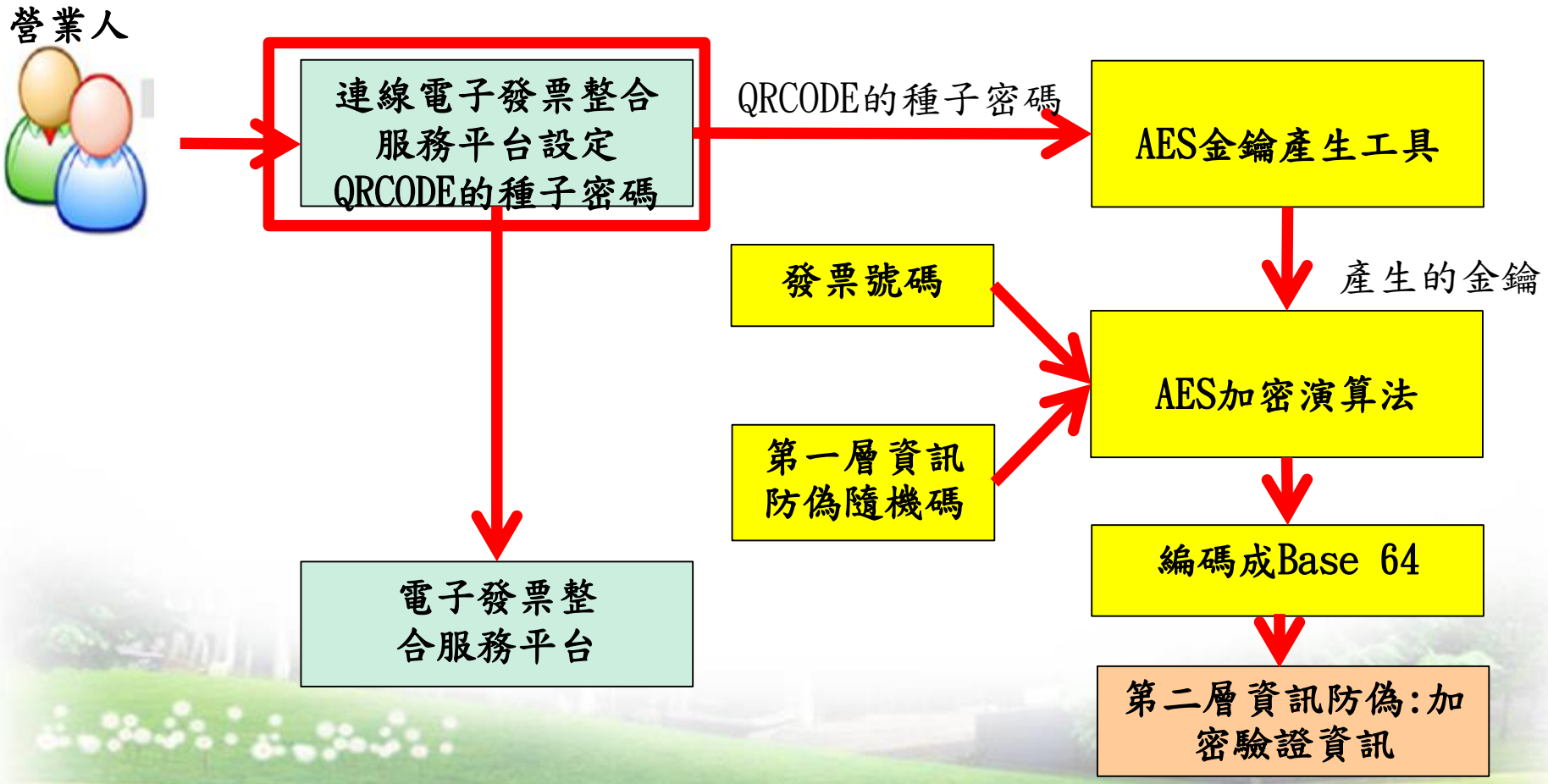
- 不定長，以「:」做為間隔符號

欄位名稱	長度	說明
營業人自行使用區	10	二維條碼若已記載完整明細資訊後，營業人可在此自行增加其他資訊。 若不使用則以10個「*」呈現。
品目總筆數	10進制	左、右二維條碼所記載之完整品目總筆數
交易品目筆數	10進制	該次交易之品目筆數
中文編碼參數	1	Big-5為0、UTF-8為1、Base64為2 。(在第一個品名前的間隔符號後的所有資訊)
品名		包含中文字，編碼規則由上述參數判斷。
數量	10進制	編碼規則由上述參數判斷。
單價	10進制	編碼規則由上述參數判斷。

- 右方二維條碼說明
  - 首2碼固定為起始符號「**」
  - 接續左方二維條碼不敷記載之編碼後資訊，若無則空白
  - 二維條碼不敷記載所有交易品目筆數時，應須能納入最多品目筆數記載

電子發票證明聯資訊防偽機制

第二層資訊防偽:加密驗證資訊產製過程



電子發票證明聯資訊防偽機制

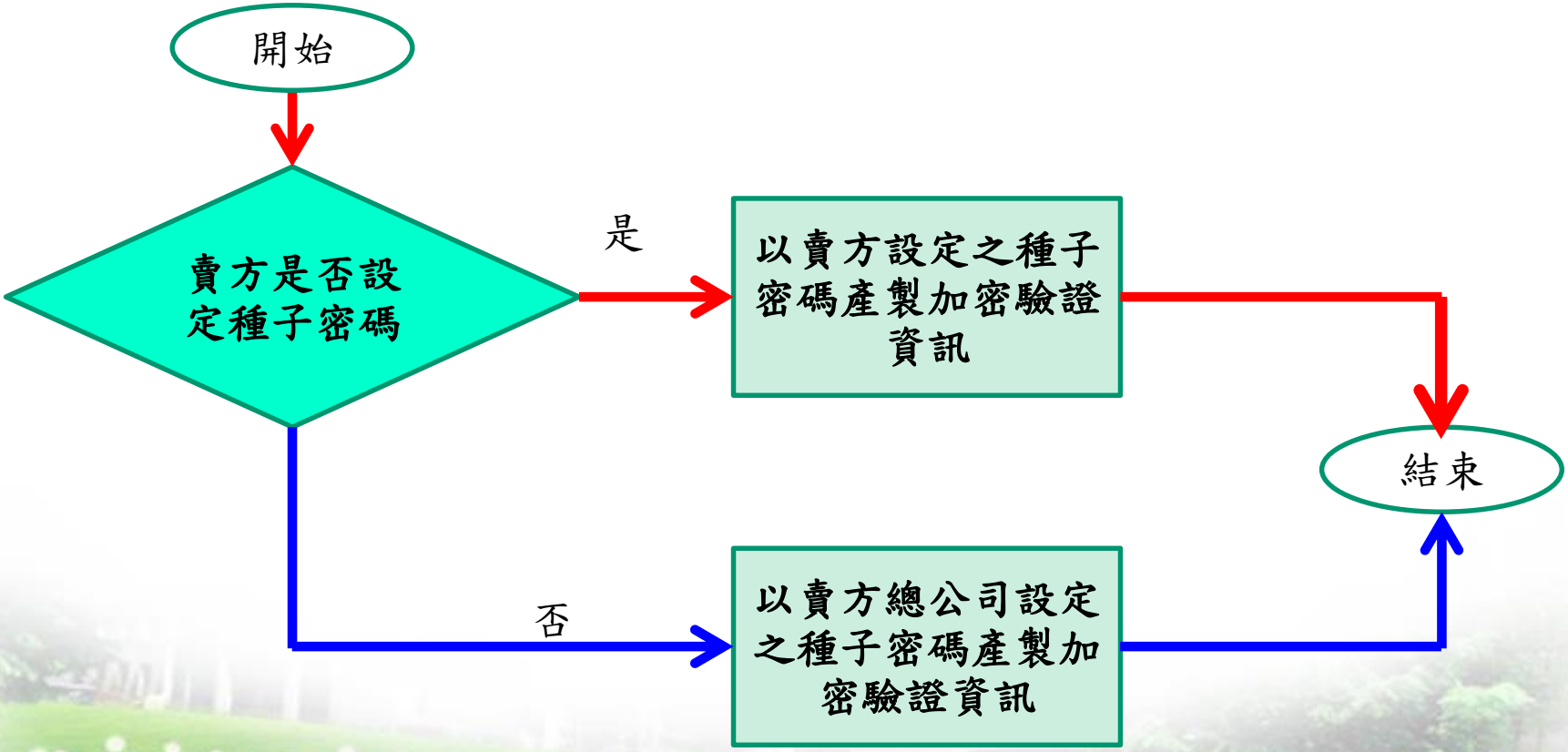
電子發票平台設定QRCode種子密碼

設定可採
1. 憑證登入
2. 密碼種子登入
兩種機制

連線電子發票整合服務平台設定QRCODE的種子密碼

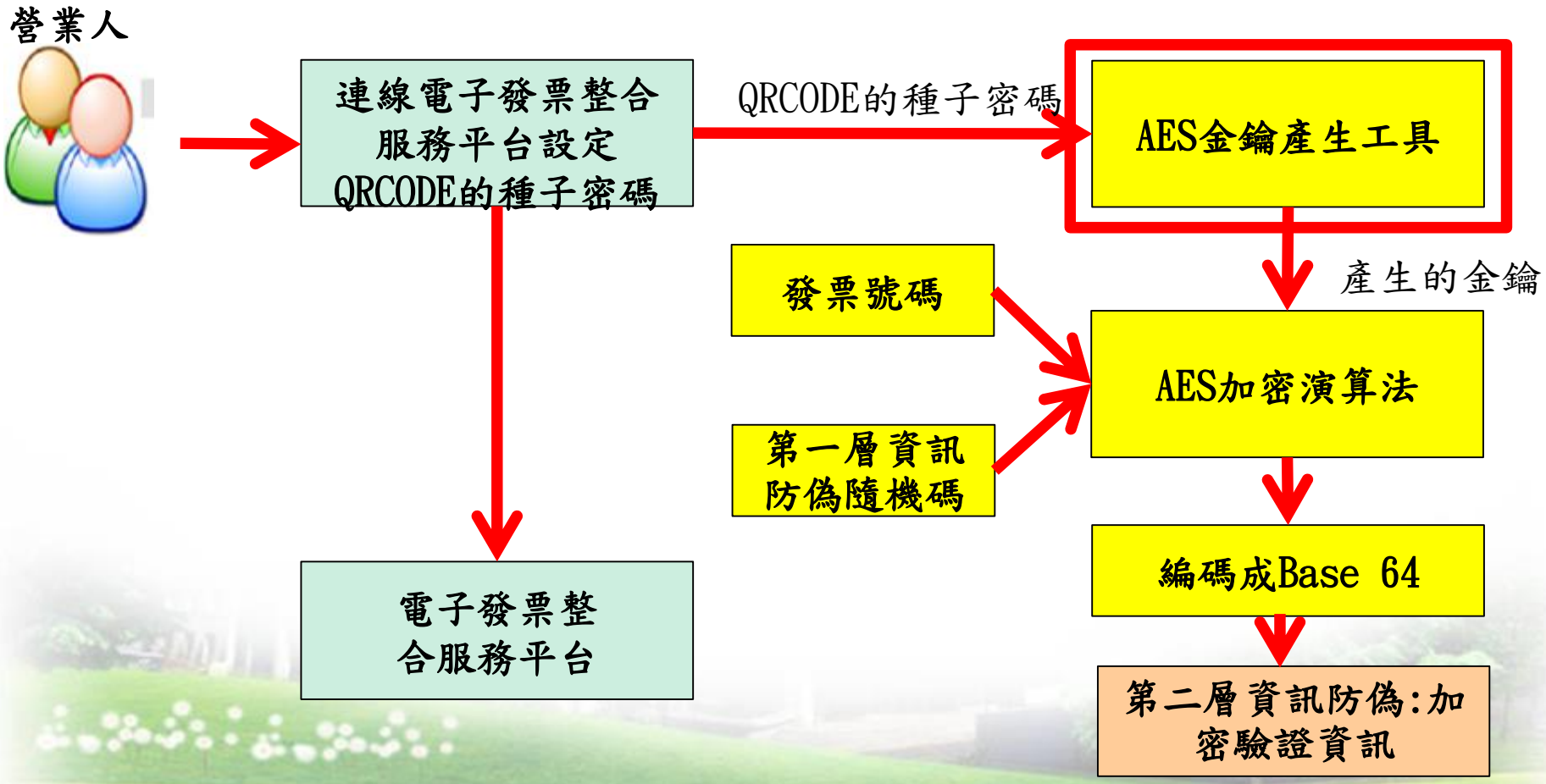
電子發票證明聯資訊防偽機制

- QRCode種子密碼決定優先順序



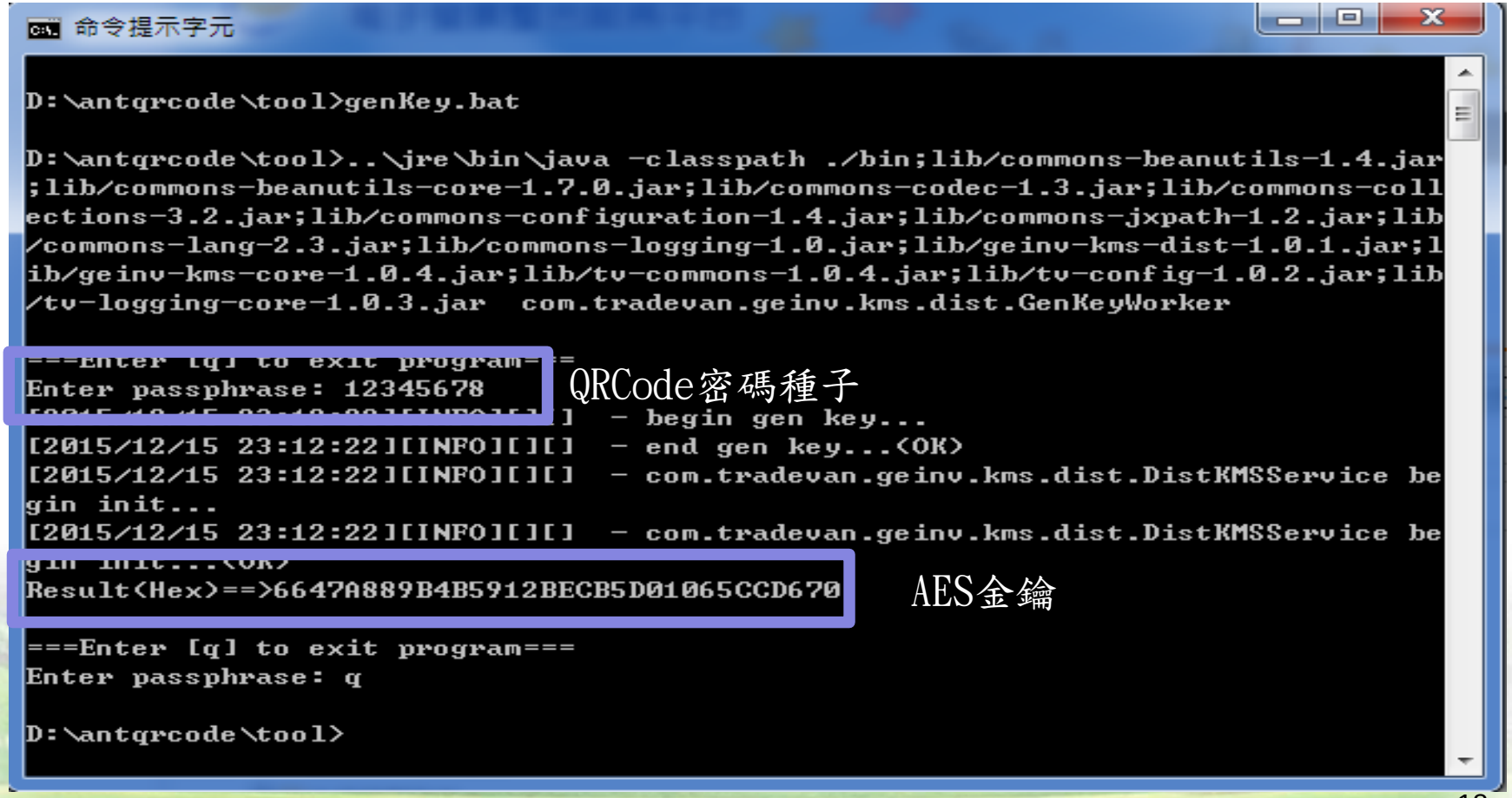
電子發票證明聯資訊防偽機制

第二層資訊防偽:加密驗證資訊產製過程



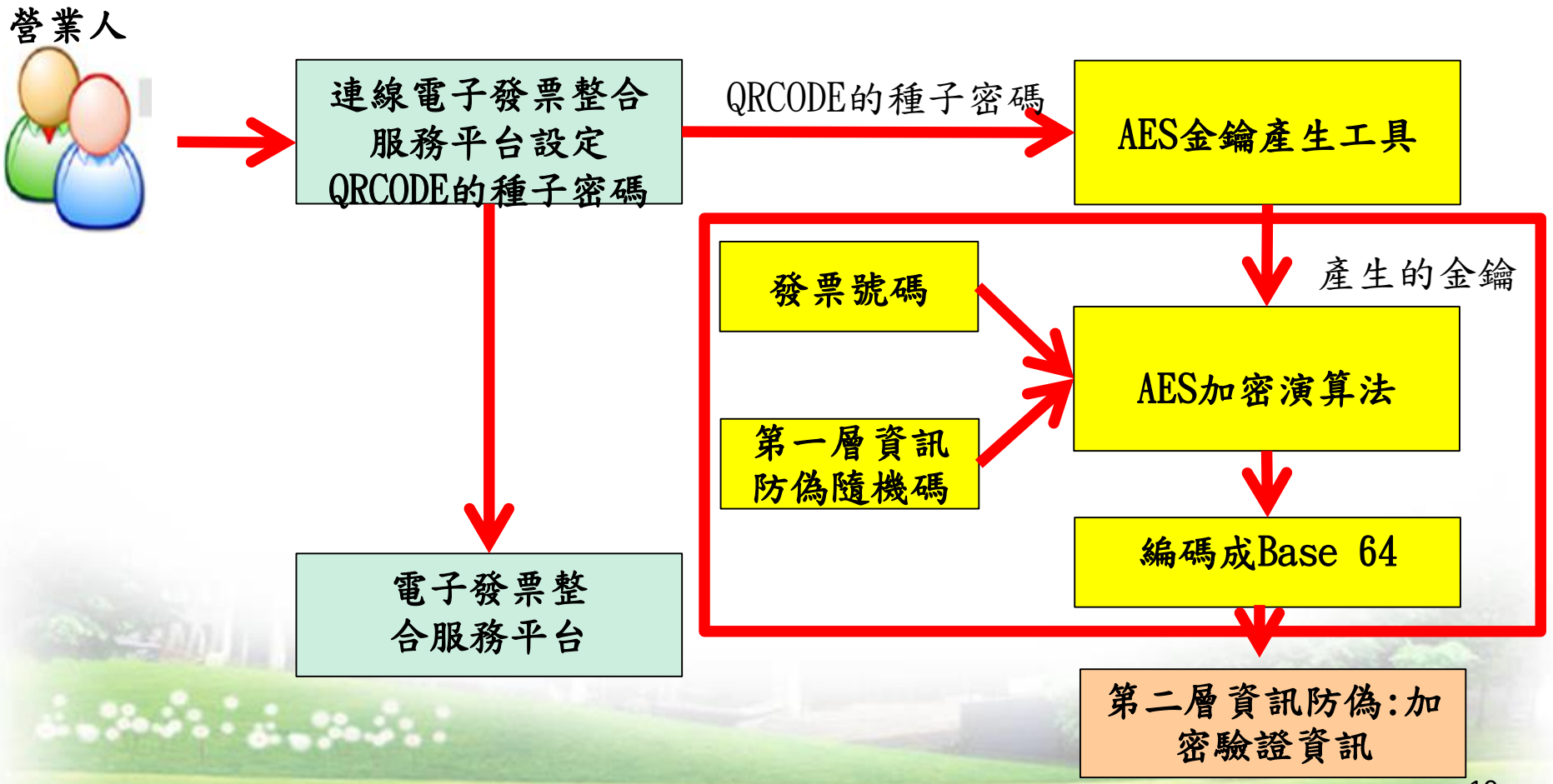
電子發票證明聯資訊防偽機制

AES產生工具產生AES金鑰



電子發票證明聯資訊防偽機制

第二層資訊防偽:加密驗證資訊產製過程



電子發票證明聯資訊防偽機制

- QRCode加密驗證產製

捲動 命令提示字元

```
Buildfile: D:\antqrcode\build.xml

clean:
   [delete] Deleting directory D:\antqrcode\build

compile:
    [mkdir] Created dir: D:\antqrcode\build\classes
    [javac] D:\antqrcode\build.xml:16: warning: 'includeantruntime' was not set,
 defaulting to build.sysclasspath=last; set to false for repeatable builds
    [javac] Compiling 2 source files to D:\antqrcode\build\classes

jar:
    [mkdir] Created dir: D:\antqrcode\build\jar
      [jar] Building jar: D:\antqrcode\build\jar\Qrcode.jar

run:
     [java] aeskey=6647A889B4B5912BECB5D01065CCD670
     [java] QrCodeString=AA12345678104121912340000000b40000000b400000000054185095dS
ypnr83S3oOPU5HiEx49w==
     [java] dSypnr83S3oOPU5HiEx49w==
     [java] AA123456781234

BUILD SUCCESSFUL
Total time: 1 second

D:\antqrcode>
```

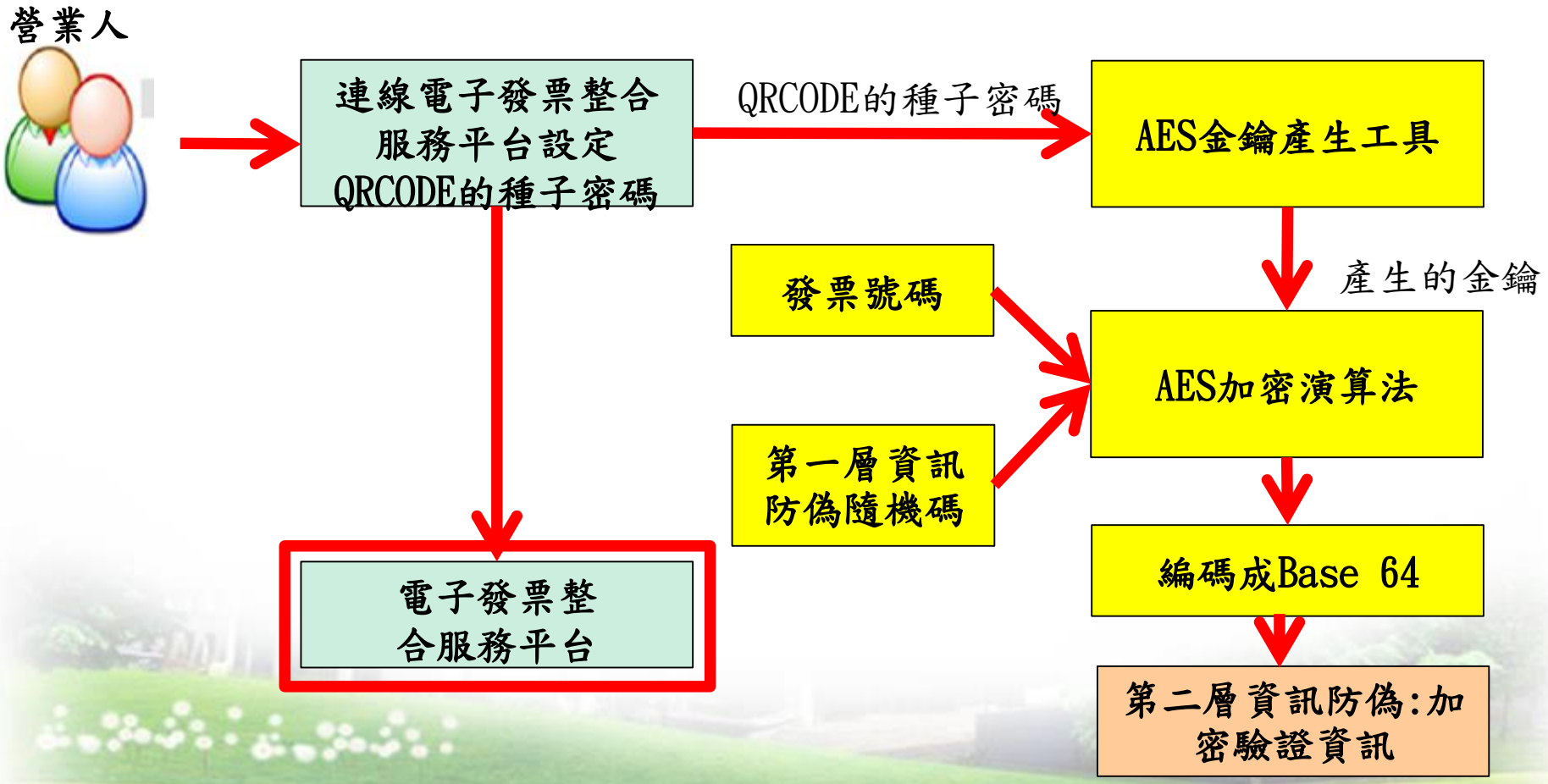
AES金鑰

加密驗證資訊

QRCode加密字串

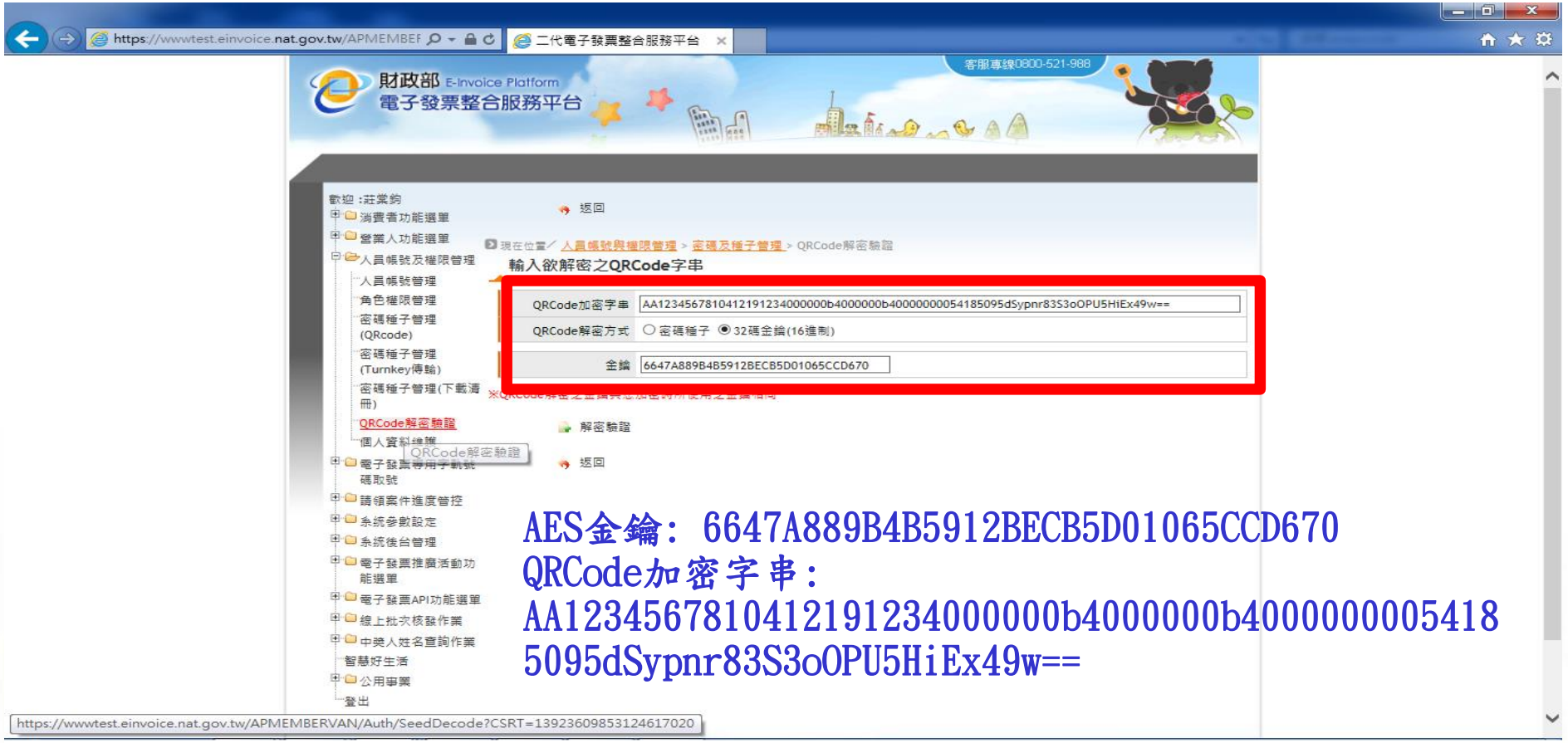
電子發票證明聯資訊防偽機制

第二層資訊防偽:加密驗證資訊產製過程



電子發票證明聯資訊防偽機制

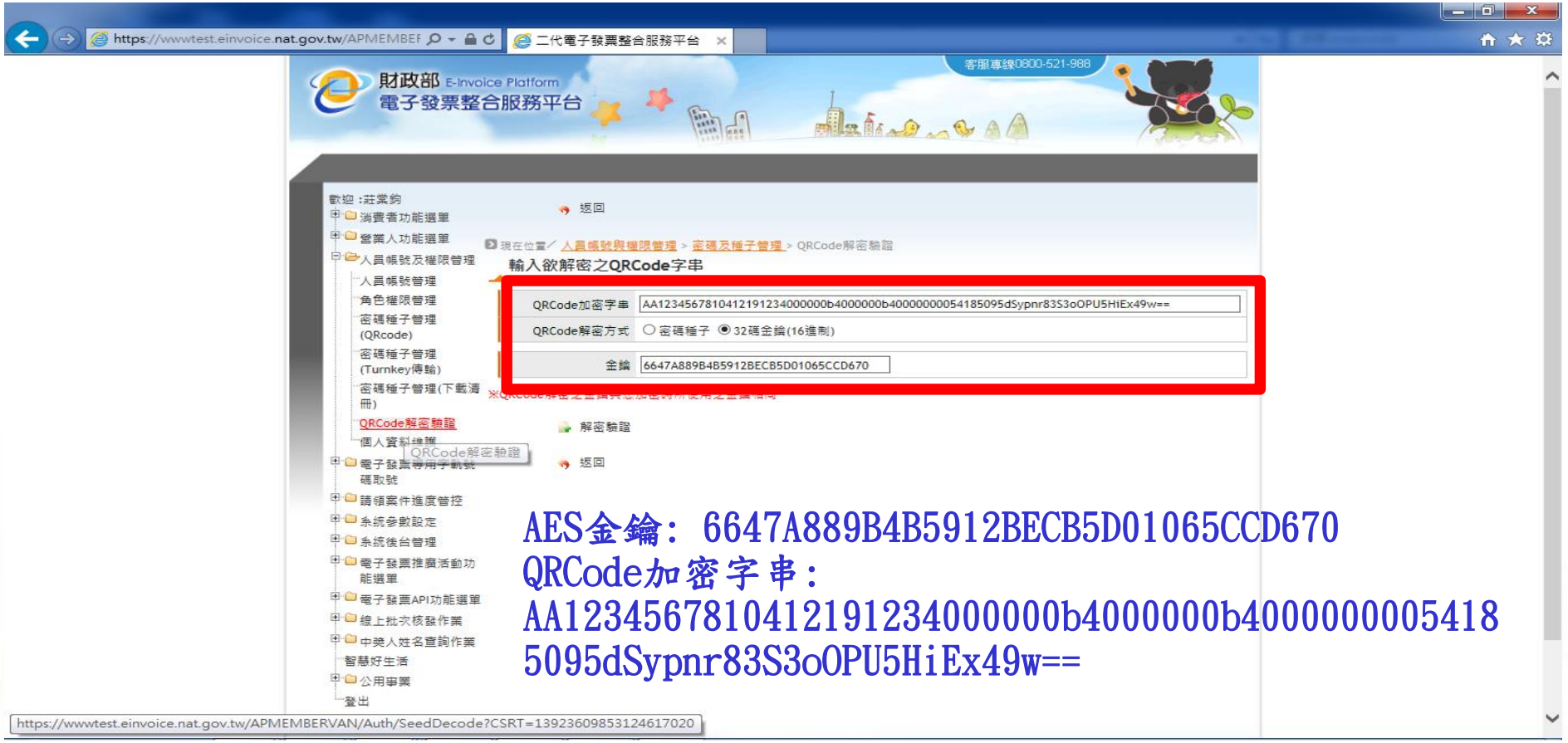
- 方法1:以AES金鑰進行驗證加密驗證資訊正確性



AES金鑰: 6647A889B4B5912BECB5D01065CCD670
QRCode加密字串:
AA12345678104121912340000000b4000000b400000000054185095dSypnr83S3oOPU5HiEx49w==

電子發票證明聯資訊防偽機制

- 方法1:以AES金鑰進行驗證加密驗證資訊正確性



AES金鑰: 6647A889B4B5912BECB5D01065CCD670
QRCode加密字串:
AA12345678104121912340000000b4000000b400000000054185095dSypnr83S3oOPU5HiEx49w==

電子發票證明聯資訊防偽機制

- 方法1:以AES金鑰進行驗證加密驗證資訊(驗證正確)

解密結果

發票資訊		明文
發票字軌：	AA12345678	AA12345678
發票開立日期：	1041219	
隨機碼：	1234	1234
銷售額：	180.0	
總額：	180.0	
買受人統編：	00000000	
營業人統編：	54185095	
密文：	dSypnr83S3oOPU5HiEx49w==	

1.紅色框框上面的欄位是發票號碼下面欄位是隨機碼，如果與電子發票證明聯一致表示驗證通過。
2.請將上面的欄位與電子發票證明聯比對:發票號碼、開立日期、隨機碼、總額、營業人統編、買受人統編(有打統編)等。
3.請與前一頁QRCode加密字串的最後面24位與密文比對是否一致。

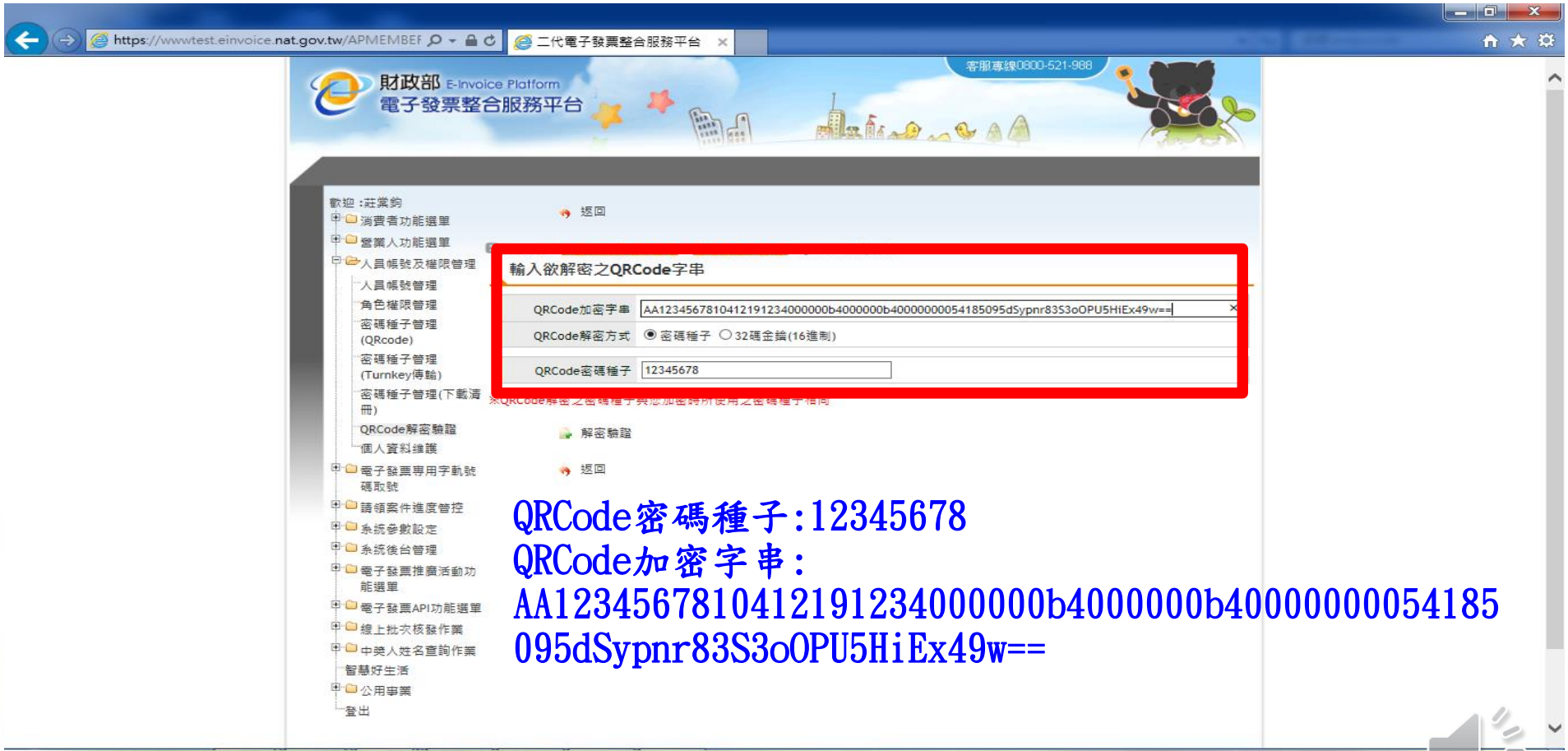
電子發票證明聯資訊防偽機制

- 方法1:以AES金鑰進行驗證加密驗證資訊(驗證失敗)

紅色框框上面的欄位是驗證錯誤非發票號碼下面欄位是驗證錯誤非隨機碼，表示驗證失敗其他都不要再檢查

電子發票證明聯資訊防偽機制

- 方法2:以種子密碼進行驗證加密驗證資訊正確性



QRCode密碼種子:12345678
QRCode加密字串:
AA12345678104121912340000000b4000000b400000000054185095dSypnr83S3oOPU5HiEx49w==

電子發票證明聯資訊防偽機制

- 方法2:以種子密碼進行驗證加密驗證資訊(驗證正確)

解密結果

發票資訊		明文
發票字軌：	AA12345678	AA12345678
發票開立日期：	1041219	
隨機碼：	1234	1234
銷售額：	180.0	
總額：	180.0	
買受人統編：	00000000	
營業人統編：	54185095	
密文：	dSypnr83S3oOPU5HiEx49w==	

1.紅色框框上面的欄位是發票號碼下面欄位是隨機碼，如果與電子發票證明聯一致表示驗證通過。
2.請將上面的欄位與電子發票證明聯比對:發票號碼、開立日期、隨機碼、總額、營業人統編、買受人統編(有打統編)等。
3.請與前一頁QRCode加密字串的最後面24位與密文比對是否一致。

電子發票證明聯資訊防偽機制

- 方法2:以種子密碼進行驗證加密驗證資訊(驗證失敗)

紅色框框上面的欄位是驗證錯誤非發票號碼下面欄位是驗證錯誤非隨機碼，表示驗證失敗其他都不要再檢查